Local Members Interest
N/A

Audit and Standards Committee - Tuesday 13 July 2021

Information Governance Annual Statement

Recommendation

I recommend that the Committee:

a. Note the information contained within the report.

Report of the Director of Corporate Services

Report

1. This report is designed to give the Audit and Standards Committee assurance how Staffordshire County Council are complying with the following legislation:

    a. Data Protection Act 2018 and UK-GDPR
    b. Freedom of Information Act 2000
    c. Environmental Information Regulations 2004
    d. Regulation of Investigatory Powers Act 2000
    e. Local Government Transparency Code 2014

2. The compliance with this range of legislation is monitored and administered through various national commissioner roles including the Information Commissioner, Surveillance Commissioner and Interception of Communications Commissioner. These commissioners have powers to impose penalties, including monetary penalties and custodial sentences on organisations or individuals who breach these rules.

Information Rights

Data Protection

3. Under the Data Protection Act individuals have a right to access their own information, known as a Subject Access Request. Ensuring compliance with Access to Information is the overall responsibility of the Information Governance Unit. However, Families First manage children's requests separately. Compliance statistics for both are included at **Appendix 1**.

Freedom of Information

4. Freedom of Information performance in SCC is monitored on a quarterly basis and published on our website. The benchmark set by the Information Commissioner for an acceptable service is 85% of requests answered with 20 working days. Freedom of Information statistics can be found at **Appendix 2**.

Information Security

5. Local Authorities continue to face challenges to ensure that appropriate information security is in place therefore the County Council remains focussed on working towards ensuring that resilient procedures are employed across the Authority. This has been updated in include the challenges from an increase in home working during Covid-19.

6. The authority continues to be subject to a high-level of cyber-attacks. It is not believed that the authority is being specifically targeted but more as an inevitable consequence for any organisation that has a high level of activity on the internet. In particular denial of service attacks have seen an increase both directly attacking the Authority's network but also that of our Internet Service Provider and this can lead to significant disruption to the network. An increase in malware email campaigns (software which is specifically designed to disrupt or damage a computer system) has led to limits being placed on downloading executable files. There has also been a rise in Ransomware attacks at a global level and a school in Staffordshire was subjected to a successful attack at the end of 2020. The IG Team worked with the ICT supplier, the Information Commissioner's Office and Action Fraud to resolve the issue. The school were not directly targeted.

7. The Council continues to update the Cyber Security Incident Plan in case of a cyber-attack. In December 2020 the council appointed a Cyber Security Manager who is responsible for ICT Security and the authority's compliance with industry and sector security standards. The Cyber Security Manager is working closely with the Information Governance Unit to improve overall security governance.

8. The Council continues to invest in appropriate software and hardware to combat security threats and works closely with its Internet Service Provider to improve its security and to ensure the earliest possible warning of cyber-attacks. The firewall hardware and software continue to provide protection to our network. The council is currently looking to invest in a Security and Information Events (SIEM) solution. A separate Cyber Security report has been written which accompanies this statement.

9. The Information Governance Unit record all reported security incidents and investigate where necessary. Security incidents include both physical and electronic data. All incidents will be followed up with the appropriate manager to receive assurance from the service that recommendations have been implemented. A total of 314 incidents were reported between April 2020 and March 2021 which is the highest level of incidents since we began formally recording. This is an average of 26 per month. 28 incidents were reported to the Information Commissioner's Office, no further action was taken. There was a rise in incidents which coincided with home working. It is believed that as more staff undertake the training they are more aware of reporting and have the confidence to report. Details of Security Incidents are also included at **Appendix 2.**

10. Staffordshire County Council has successfully been granted Public Services Network (PSN) accreditation for 2021. PSN is a key part of Government ICT

Strategy and accreditation means that the authority can continue access a secure network that facilitates the safe access of Government shared services. The safety of PSN is paramount and to achieve accreditation the authority had to satisfy a Code of Connection containing over 60 different security controls. This included an externally procured Pen test carried out in 2020 where there were no critical or high actions.

11. Staffordshire County Council has also been accredited with Cyber Essentials Tier 1 for the third year running.

Governance

12. Governance of information requirements is provided through the Corporate Governance Working Group, Information Governance Unit, Senior Information Risk Owner (SIRO) Data Protection Officer (DPO) and two Caldicott Guardians.

13. An Information Asset Register (IAR) identifies information that enables the organisation to perform its business functions and all rules associated with the management of that information. Further work to improve the IAR recording process is being undertaken.

14. Staffordshire County Council has a comprehensive retention schedule, which identifies the statutory and business requirements for how long a record should be kept.

15. The NHS IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards. The NHS require the County Council to be compliant with the toolkit to enable integrated working between the County Council and NHS bodies, including connection to systems and the transfer and sharing of sensitive personal data. In March 2020 Staffordshire County Council obtained compliance to the latest local authority version of the toolkit for the whole County Council.

Information Management Strategy

16. The Information Governance Team has developed an Information Management Strategy and Framework. The strategy will run between 2021 and 2024 and is designed to support every member of staff with their individual responsibilities regarding the processing of personal data.

17. A working group of stakeholders has been formed which includes, DPO, SIRO, Caldicott Guardians and Information Asset Owners. The group meet monthly with a key responsibility being to promote and embed the strategy within their own areas and highlight any risks and mitigations that need to be taken into consideration.

18. The framework can be found at **Appendix 3.**

Training and Guidance

19. All new starters must complete the, Data Protection and Cyber security e-learning modules as part of the induction process. All staff are also recommended to complete a suite of Information Governance e-learning modules.

20. The DOJO videos have been rolled out and a further set of videos designed for members were released in March 2020.

Regulation of Investigatory Powers Act (RIPA)

21. Staffordshire County Council is entitled to use the Regulation of Investigatory Powers Act for carrying out covert surveillance as part of our statutory duties. All applications for surveillance must be approved by a Magistrate. In 2020 there were 0 Directed Surveillance applications made. No operations involving Covert Human Intelligence Sources were undertaken.

22. Access to Communications Data from communication are processed by the National Anti-Fraud Network (NAFN). No requests have been made or processed. A new Code of Practice has been issued and further work is underway to ensure compliance with the new code of practice.

23. Several RIPA training sessions have been delivered, over the past 12 months An updated RIPA policy alongside new guidance on the use of social media for investigations has been published. A RIPA inspection was carried during 2020, and the 7 areas of improvement have all been addressed.

24. Following a national audit by the Surveillance Commissioner's Office, further work has been untaken to ensure all CCTV devices managed by the council are accounted for and managed in line with the Code of Practice.

Equalities Implications

25. There are no equalities implications arising as a result of this report.

Legal Implications

26. Failure to comply with legislation or legal requirements (i.e. Data Protection Act, Regulation of Investigatory Powers Act) can result in external censure, financial loss (including fines and compensation) and reputational damage.

27. Failure to comply with the Regulation of Investigatory Powers Act can result in censure by the Surveillance Commissioner, including reporting to Parliament, and judgement by the Investigatory Powers Tribunal.

Resource and Value for Money Implications

28. Continued adherence to good information assurance practice will help to ensure that the Council does not suffer financial loss through fine(s) for breaches.

Risk Implications

29. Any risks identified are subject to inclusion within the Authority's risk register and are dealt with as a matter of priority accordingly.

30. It is a key part of the Committee's role to give assurance to the Authority and the council taxpayers that the public resources invested in the Authority are being properly managed. This report is one way by which that assurance can be given.

Climate Change Implications

31. There are no climate change implications arising as a result of this report.

List of Background Documents/Appendices:

Appendix 1: Subject Access Requests
Appendix 2: Freedom of Information Requests, Information Security Incidents
Appendix 3: Information Management Framework

Contact Details

Assistant Director: Tracy Thorley, Assistant Director for Corporate Operations

Report Author: Natalie Morrissey
Job Title: Information Governance Manager
Telephone No.: 01785 278314
E-Mail Address: natalie.morrissey@staffordshire.gov.uk